EPRI

Point of View

The Y2K transition and related problems may be a preview to other microprocessor incompatibilities in the new millennium. Electromagnetic compatibility (EMC) is emerging and will be an important area of research to better understand why microprocessor-based electronic systems aren't performing under some critical conditions.

In the words of a prominent utility executive, "EMC is a real and continuing challenge. Today's competitive environment demands that we have more economical and effective methods for finding and eliminating the sources of interference."

The electromagnetic environment that may affect microprocessor controls and other electronic systems consists of low-frequency (60-Hz and harmonics) electric and magnetic fields, which originate from normal operation. It also includes higher frequency electromagnetic fields, which come from less normal operations and events, such as switching transients, faults, their related emissions, and surges from lightning. Even distribution line corona- and arc-related discharges can upset nearby electronic appliances. And most of today's energy service personnel

Countdown to the Millennium

UPS Manufacturers Say They're Ready

The North American Electric Reliability Council (NERC) expects the transition through critical Year 2000 (Y2K) dates to have minimal impact on electric system operations in North America. In April NERC reported to the U.S. Energy Department that the electric power industry has completed 75% of the testing and preparation necessary for the Y2K transition—up from 44% in November 1998. Furthermore, most potential Y2K-related problems will have been identified and fixed by June 30, 1999. The few that miss this date will not pose a threat to the electric grid. Devices that do experience trouble with date manipulations exhibit mostly nuisance errors, such as incorrect date displays and date-time stamps.

Even so, customers are examining the efforts of energy providers to ensure a smooth Y2K transition. Under even greater scrutiny are the manufacturers of equipment designed to provide critical backup power, such as uninterruptible power supplies (UPSs).

Signature recently spoke with Steve Crow, Best Power; Tony DeSpirito, American Power Conversion (APC); Darrick Finan, Powerware (formerly Exide Electronics); and Tom Gruzs, Liebert, to gather their collective intelligence on the matter.

What do your customers tell you they need to prepare for Y2K?

Finan: At Powerware our customer calls are all over the map. There are the simple requests: "Is my power protection equipment Y2K-compliant, and will it work after January 1, 2000?" Then there are other customers, like Lucent, who sent a 100-page questionnaire and followed up with a conference to discuss it, line by line. On one hand, they are verifying the compliance of our products; on the other, they are assessing their internal systems and wondering, "Will the badge reader work, so we can get into the building in January?"

Gruzs: Liebert's precision air conditioning, power conditioning, and UPS systems support critical,

computer-supported loads, such as data centers. Our customers are giving us close scrutiny because they depend on our products for continuity of electric power supply. As part of their preparedness, they are looking to all of their suppliers to ensure Y2K compliance.

DeSpirito: At APC we've found customers are looking at their operating system applications first—the hardware that an application runs on, the power protection equipment, and the infrastructure supporting that equipment. They want assurances that power from energy providers and inside the building won't be cut off as a result of Y2K. Our products take care of the information technology hardware and customer applications running on the hardware.

Banking is one of many industries that will rely on UPSs for critical backup power, if needed, during the Y2K transition.

Crow: At Best Power the majority of our business is related to providing power protection to computers and telecommunications equipment. We get a lot of requests for letters of compliance on our products, especially from the banking and healthcare industries. The biggest concern we hear is that people are afraid their computer-driven equipment will shut down as a result of Y2K. They need reassurance that it won't happen.

What problems are your customers anticipating?

DeSpirito: That's the $64,000 question. Some are anticipating a blackout on January 1, 2000. Some are anticipating absolutely no change in function whatsoever. If I were to characterize the general mood, I'd estimate that the majority does not expect a disruption in

It is important to check the Y2K compliance of any building or manufacturing system that uses embedded microprocessors.

power to critical systems. They are fairly confident that the electricity infrastructure is Y2K-compliant. APC maintains relationships with energy providers to help address Y2K and a host of power quality issues. Most recently in April we established a strategic alliance with Select Energy to increase power availability throughout the Northeast.

Finan: Everyone has heard the gloom and doom about Y2K. But to assess the impact on their equipment, they need to ask, "What is this equipment doing, and why would it be date-sensitive?" If they are using a UPS simply to back up power supply, then Y2K is not an issue. But if it's being used to do automatic shutdowns on a periodic basis, then they either need to ensure that the UPS is Y2K-compliant so things happen as scheduled, or they should avoid critical times like January 1, 2000, and give themselves time to react.

Customers should also keep in mind that hardware and software compliance are two different things. UPSs are not required to have a lot of intelligence, so most of the hardware has no date sensitivity. But 90% of UPSs sold in the world today use software. The customer

Courtesy of American Power Conversion Corporation

needs to ask, "Am I using software provided by the manufacturer?" And if so, "Is it Y2K-compliant?" Finally, when they call us at Powerware, it helps to have specific information about their unit, ideally the serial number.

Crow: Most customers are expecting minimal problems from the power industry relating to Y2K. They are taking proactive steps to identify and rectify any potential problems ahead of time.

Gruzs: Rather than anticipate problems, they're hoping to eliminate them. We have many people at Liebert making sure that our customers are prepared. We have answered thousands of questions on our equipment's ability to withstand the Y2K transition. Even so, the majority of our large users are requesting that we provide them with a dedicated, on-site service person on December 31. While there are human resource limitations, we will provide this service whenever possible.

As a side note, it's interesting that the public is so focused on January 1, 2000, as *the* date that could create problems. There are others, including April 9, 1999 (the 99th day of the 99th year), which passed smoothly; September 9, 1999 (9/9/99); and February 29, 2000 (leap year).

Also, with the International Date Line in the Pacific Ocean, we in the United States will be among the last to see midnight—and the impact of Y2K on our computer-controlled systems. Unless the power goes out,

we will be able to watch and see if there really is a Y2K bug. I'd say the biggest risks for problems are in developing countries, which are a major market for old computers and have not spent as much money on Y2K preparations.

How are you helping customers address Y2K concerns?

Crow: The Best Power Web site details the Y2K compliance of our products. Written test procedures for each product family are also available on the Web, so our customers can run tests themselves. If a customer requests certification of a particular unit, we will send a letter that states the unit has passed compliance testing. And if a customer wants on-site testing of our product, our worldwide service center can provide that service.

Gruzs: We have run tests on all Liebert equipment, and our Web site contains our compliance statement. When customers require demonstrations of compliance, we will make site visits and run the Y2K tests again. Our business systems have been verified for Y2K readiness, an effort that was started in 1995.

Finan: We're providing Powerware customers with intelligence and feedback on where our components fit into the Y2K compliance picture. First, with UPSs generally not being the most intelligent beasts on the market, hardware compliance is not an issue. As far as the software, we started working early in 1998 to

How Ready Are We?

by Miles R. Walbrecht

The Y2K computer date issue has made one thing abundantly clear: Ours is a highly complex and interconnected world. It seems that everything from personal computers to manufacturing controls and vast telephone switching networks have date coding that could bring down a computer system.

Although estimates indicate that less than 1% of today's computer software or firmware may have Y2K-related problems, there remains a high probability that many of our computer-based systems remain vulnerable. Supplying electric power to our homes and industries, for example, depends on the continued functioning of a multitude of services. At the heart of these services lies a "nervous system" of computerized control, reporting, data processing, and administrative management functions. The computers contain software that, in many cases, has evolved from the early 1960s, with date standards and functions that are still not uniformly applied.

Questions of Supply

To illustrate the interconnectivity of our society, let's look at a portion of the supply chain for generating electric power from coal. Just getting the coal from the mine to the power plant involves several linked activities that must function in harmony.

The coal must first be mined and then loaded onto trains. The train locomotives must have diesel fuel;

the fuel must be refined; refineries must have crude oil; and the crude oil must be pumped, collected, and transported. Once the trains start to roll, traffic scheduling and routing must function properly. All of these are major enterprises that rely on computer-managed administrative and Supervisory Control and Data Acquisition (SCADA) equipment and software, which in turn depend on reliable telecommunications and electric power.

The problem with any chain is that a failed link can bring down the entire system, unless there is a parallel redundant link to carry the load. The railroad system, for example, may not have adequate redundancy, since a few stalled trains can back up and paralyze the system.

Because about 40% of the electric power generated in the United States uses coal as an energy source, it is possible that a significant number of power plants could run out of fuel before supply problems can be corrected. So the question becomes, "Can the electric power industry continue to supply reliable, high-quality power to its customers after 2000?" No one knows the answer. Even if the industry is fully Y2K-compliant, what will be the status of its suppliers?

Energy Service Ramifications

Beyond these issues are the power quality problems that could surface during power delivery. While some customers can tolerate slight voltage disturbances, others cannot. Engine generators and uninterruptible power supplies can mitigate short-term problems, but

Supply shortages could result if Y2K affects any aspect of railway system operations.

such resources generally are not available to most industries and private customers.

Once again, the continuing function of computer-controlled SCADA systems becomes critical. Without SCADA, power system operators and dispatchers would have great difficulty in manually monitoring and controlling the various devices that govern the generation and delivery of electricity. Since many of these monitoring devices are scattered over large distances, telephone and data lines are also crucial to power system management.

Finally, there is the question of whether enough technical people will be available to correct the computer control and monitoring problems that could occur during the Y2K transition. Such repair is often tedious and time-consuming under the best of circumstances. It is not too far-fetched to envision our energy service providers being overwhelmed with these kinds of problems, especially in the new environment of separate suppliers, transporters, and retailers of electricity.

Contingency planning and implementation are the only options left in the event that key supplies and services are disrupted. Reports have surfaced that many energy providers are stockpiling fuel and other necessary resources, that repair crews will be on alert, and that excess generating capacity may be placed on-line.

But when one considers that there are more than 15,000 utility and nonutility generating units with a wintertime generating capacity of over 750,000 MW—of which about 40% use coal to supply power to an untold number of interconnected distribution systems—one can see that an enormous job awaits us in the remaining months of 1999. So, let's get on with it and finish our work. ■

Miles R. Walbrecht is an engineering program manager at Conwal, Inc. (*walbrech@erols.com*) in Washington, DC. He assisted the Federal Aviation Administration in replacing and expanding the critical power system at its 21 air route traffic control centers.

Y2K 101

Signature interviewed Alex McEachern, director of WPT, the parent company of Dranetz-BMI and Electrotek Concepts (*http://www.dranetz-bmi.com/*) in Emeryville, California, to uncover the basis for potential Y2K problems.

What is it that makes the Y2K computer date problem so difficult to nail down? At first glance, the problem may appear easy to understand, but it actually involves several subtle layers. It is also ubiquitous, occurring in almost all equipment built before 1990 that operates at the command of embedded microprocessors.

Embedded microprocessors are the computers-on-a-chip that are built into all kinds of products, ranging from fax machines to gas pumps to electricity monitoring equipment, according to McEachern. Just like any other computer, microprocessors rely on software to tell them what to do. This software—or firmware, which is what software stored in hardware is called—is usually stored as a long series of data bytes on Erasable Programmable Read-only Memory chips, or EPROMs.

As firmware is written in a language like "C" on a personal computer (PC), a program on the PC compiles the "C" program into a series of data bytes. The PC transmits these bytes via cable to a tool called an EPROM programmer, which "burns" the bytes into the EPROM, which then can be plugged into a socket on the microprocessor. If everything works properly, the microprocessor starts running the program—and can do so for years.

Typical Problems

"At Dranetz-BMI, we have been shipping microprocessor-controlled instruments for more than 20 years," says McEachern. "We've solved all of our Y2K issues, and you can download certificates of compliance from our Web site. But we did find a couple of surprises along the way."

The standard explanation is that Y2K bugs exist because the programmer tried to save memory by storing the year in just two digits. "But it's actually more complex than that," says McEachern. For example, firmware engineers typically move to new jobs every few years, and many Y2K problems were created back in 1986 and 1987. So, a new engineer has to become familiar with the complicated creation of an engineer who is no longer available.

Also, the tools for modifying the firmware are often changed. The programs themselves have been carefully archived, stored in vaults, and backed up regularly. But the EPROM programming tools get revised every year or so and lose compatibility after a few generations. "It's as though new wrenches came out every year," says McEachern. "That would make it difficult to work on a 12-year-old bolt."

Y2K Bug Origins

So, what is a typical Y2K bug? McEachern offers this example: Back in 1986, an instrument was programmed to ask the user to punch in the month and year of the
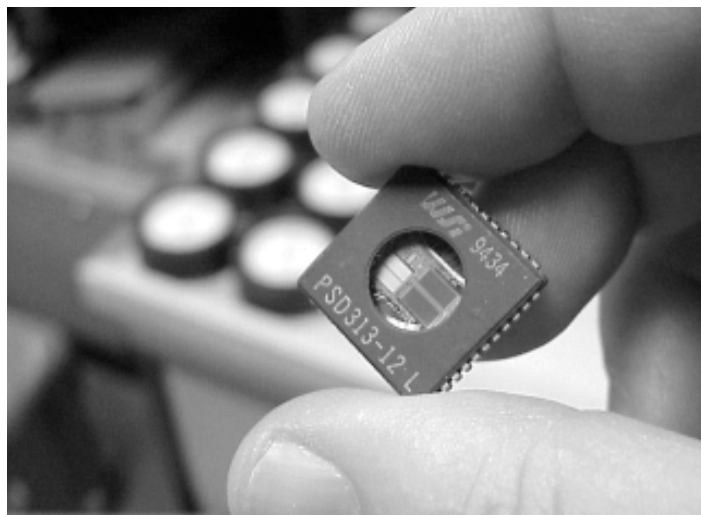
The firmware in a microprocessor is stored on an EPROM. Disks would be too big, too expensive, and too fragile.

instrument's next scheduled calibration. The instrument carefully verifies that the month entered is between 01 and 12, inclusive, and that the year is two digits and greater than 87. It made sense at the time, and it worked perfectly for 14 years. But, if the user enters a calibration date in the year 00, the instrument rejects it because the computer sees 00 as lower than 87. "We had to issue new EPROMs for that one," says McEachern.

Here's another example: A monitoring instrument creates disk files and names the files based on the date, so a file created on January 4, 1992, is called "04JAN92." The instrument will work just fine after 2000. For example, files created on February 15, 2002, will be named the six-character "15FEB2." But, as it turns out, the software on another embedded microprocessor assumes that file names are exactly seven characters long, and behaves in an obscure but unpleasant way when they aren't. Again, new EPROMs are required. Fortunately, once a problem is found, it's a simple matter to unplug an old EPROM and plug in a new one.

There also was a widespread belief among computer programmers in the mid-1980s that, as a centennial year, 2000 would not be a leap year. (McEachern admits to making that mistake himself back in 1983.) However, as a millennial year, 2000 is a leap year. There may be some interesting Y2K problems on February 29, 2000, as well as on January 1.

"Check the Web sites of your suppliers," recommends McEachern. "Responsible suppliers will tell you about the products with problems, and they will tell you how to fix them. They will also offer certificates of compliance, and will tell you about their test procedures."

McEachern suggests being skeptical of companies that make simple, blanket statements of having no Y2K problems in their equipment—the problems are often subtle and require extensive testing. A lot of those boxes will need to be opened up and have new EPROMs plugged in before December 31 rolls around. ∎

test and verify compliance. We have a Y2K section posted on our Web site, so customers can see if their equipment is compliant. If they require a software upgrade, we supply it—and can even do it over the Web. Our software provides access to the serial number and type of UPS it supports—helping us manage our products and customers, while providing information that customers can use to manage Y2K and their growing UPS networks. We are also training our sales organization so they can articulate the Y2K issue with customers and ease their concerns.

DeSpirito: At APC we also have tested all of our equipment, and we provide a Y2K readiness disclosure on our Web site. Beyond that, we offer our Y2K PowerAudit program to help our enterprise—or largest—customers prepare their infrastructure for Y2K. In the audit,

we conduct an infrastructure analysis, identifying by manufacturer, make, and model any systems that may have compliance issues. For example, building systems such as elevators may not function if their embedded processing technology is not compliant. Systems used in the manufacturing environment—such as HVAC, lighting, and supervisory control—also have embedded processors that may be susceptible to Y2K. We tell the customer which systems are vulnerable and will get Y2K documentation if they want.

How have you adapted your products in light of Y2K?

Gruzs: Some of our preparations at Liebert took place a long time ago, when we started looking at the clock and calendar functions in our equipment. In the last couple of years, we have been running tests to verify the Y2K compliance of our

equipment. In some cases, when we found products did not comply, modifications were completed. These were essentially in the alarm and reporting functions of monitoring systems. For all software issues, we offer an upgrade path with incentives to facilitate the upgrade.

Crow: When we evaluated Best Power products for Y2K compliance in 1997, we found minimal issues in date-related reporting functions. These issues have been resolved, even though they would not have affected product operation.

DeSpirito: All hardware being shipped by APC is Y2K-compliant, as are the latest versions of our software. We are providing free upgrades as required for any old versions of software.

Finan: Our compliance efforts at Powerware have been aimed primarily at our software. Our products support 20 different operating systems, and we've made sure that all of our products understand and work with Y2K. They can all handle the four-digit date code, and with just a little tweaking, any date is easy to accommodate.

As a global company, we have also made investments to ensure the compliance of our internal systems, such as order entry, manufacturing, and invoicing. We are making sure that our suppliers can provide us with their products in 2000, because no matter how

Y2K-complaint we are, if we can't get the supplies we need, we're still out of business. We're finding that most suppliers have identified some areas in need of work, and that the most critical systems—including electric power supply—have already been brought up to compliance. Y2K is a big issue in the power industry, and most energy providers have been way ahead of the curve in making sure their systems will be up and running through the Y2K transition. ∎

Steve Crow is connectivity product manager at Best Power Corporation (*http://www.bestpower.com/*) in Necedah, Wisconsin. He specializes in the development and implementation of UPS software solutions.

Tony DeSpirito is director of global services at American Power Conversion Corporation (*http://www.apcc.com/*), and is based in Rhode Island. He manages service and support for all APC products installed in North America.

Darrick Finan is director of product marketing at Powerware Corporation (*http://www. powerware.com/*), and is based in Raleigh, North Carolina, and San Diego, California. He manages the company's Small Systems Group, which specializes in single-phase systems and software.

Tom Gruzs is applications engineering manager at Liebert Corporation (*http://www.liebert. com/*) in Columbus, Ohio. He is responsible for the environmental, UPS, and power conditioning product lines.

Continuous power is essential to the daily operation of mission-critical components, such as those used by the Federal Aviation Administration.

Courtesy of Powerware Corporation

Protecting Against Y2K Liability Exposure

by Barry J. Fleishman, Esq.

We are well into the latter stages with respect to dealing with Y2K issues. In the electric power industry, most energy providers recognize and are dealing with potential Y2K-associated problems, including power quality and reliability concerns. But if these problems indeed do take their toll, who will pay the costs?

When legal jargon is stripped away, the basic questions in most lawsuits alleging liability for damage or harm are, "What went wrong?" and "Who, if anyone, is responsible?" Cases involving potential Y2K liability ultimately will involve these same questions.

Judges and juries will determine what went wrong by trudging through the testimony of numerous engineers and computer experts, and arriving at a story that makes the most sense to them—technically referred to as "findings of fact." They then will decide who is responsible by applying legal standards to those findings of fact and determining whether people acted reasonably under the circumstances.

The issue of "reasonableness" is not as esoteric as it might seem. Legal precedent, combined with the practices of others in similar circumstances, provides a basis to assess whether a defendant breached a duty of care that resulted in damage to others.

Y2K Responsiveness List

Following are the "Top 10" ways to identify factors that will influence cases asserting liability for damage or injury resulting from Y2K problems. The extent to which any of these "responsiveness" activities applies will vary by company, but compliance with each item should be evaluated.

Y2K-related lawsuits are bound to occur in the new millennium. Proactive measures taken now can reduce liability exposures.

1. *Early Recognition and Response to Problem*. Some industries began responding to the Y2K problem five or more years ago. The time taken between recognizing a problem and giving it attention may establish whether the energy provider was delinquent.

2. *Cooperation With Governmental Regulators*. Certain industries, like the electric power industry, must meet government regulations with respect to Y2K compliance. Not observing those rules, or failing to cooperate with governmental authorities, will be used to establish breaches of good faith and reasonableness.

3. *Compliance With Industry Standards*. Similarly, many industries are taking steps to assure Y2K compliance. Although formal standards have not been set for the power industry, clear guidelines do exist. Failure to meet those stated expectations will present an initial picture of culpability.

4. *Thoroughness of Assessment*. An energy provider's assessment of its Y2K problems should be both wide and deep. Damage or injury resulting from a power disruption that could have been avoided if a more thorough investigation had been conducted could result in a finding of negligence and liability.

5. *Adequacy of Remedial Activities*. Similarly, there must be appropriate response to problems found during an investigation. Inadequate remedial or mitigation activity in the face of known problems likely will result in liability. Also, finders of fact rarely forgive cheapness. If a known problem causes damage or injury because insufficient funds were allocated to fix the problem, liability likely will result.

6. *Degree of Contingency Planning*. Bad things happen no matter how careful one may be in seeking to prevent them. Energy providers should understand this and have adequate contingency plans in place to respond to power disturbances.

7. *Disclosures to Potentially Affected Persons*. Those who could be affected by power problems should be kept informed of their exposure. Customers, third parties, stockholders, and others all need to know if they face risks so they can take adequate precautions. A failure to communicate is potentially both bad business and a breach of reasonableness that can result in liability.

8. *Requirements for Contractors*. Energy providers that rely upon the performance of others—such as distribution and transmission companies depending on power generators and grid operators—need to verify that their suppliers take proper steps to avoid Y2K problems. Closing one's eyes to the impact that others can have on business can rise to the level of negligence and result in liability.

9. *Clear Lines of Authority and Responsibility*. An improper management structure can result in a finding that an energy provider has not acted reasonably under the circumstances. Those with the authority

Sun Sets Its Sights on Y2K

by Dennis Symanski

With installations of information technology hardware and software products throughout the world, Sun Microsystems is approaching the Y2K transition with care. We are taking prudent and necessary steps to address three key areas of our business that could be affected by the date change to the new century and millennium: our retail products, internal business operations, and manufacturing capability.

To uphold good customer relations, we have undertaken an internal testing and qualifying process to make sure that all Sun hardware and software produced since May 1, 1997, will not generate errors in date data related to the year change from December 31, 1999, to January 1, 2000, as well as in leap years. As products are evaluated, we add the findings to the "Year 2000 Product Compliance Status List" on our Web site.

Assessing Operations

To ensure smooth business operations, we are evaluating the effect of the Y2K rollover on our internal systems. We have planned for extensive database backup and archiving of all files. We have also inventoried Sun's 352 business sites and assigned a priority to each.

"Mission-critical" sites include our manufacturing facilities, service call centers, company headquarters, and engineering design campuses. We are running Y2K tests on all systems at these sites, even if the manufacturer has already done its own testing. Our goal is to have every critical system Y2K-compliant by June 30, 1999.

"Mission-important" sites are those like our large sales office in New York City, which is co-located with a service center. For systems at these sites, we will accept the Y2K test results of the manufacturer. We are cross-referencing our model numbers on equipment such as uninterruptible power supplies and switchgears with the manufacturer's list of Y2K-compliant equipment.

"Low-impact" sites—such as small sales offices in Singapore and South Africa—while important, would not impact our overall operation if they lost function. We maintain a checklist of things to watch out for at these sites.

Forging Alliances

To maintain the continuity of our manufacturing operations and reduce the possibility of disruption to the goods and services we receive, we are canvassing each of our major suppliers to determine if their operations are Y2K-compliant. For example, we have been working with Liebert Corporation to ensure the compliance of the electronic controls on their power and air conditioning equipment.

We also have been in discussions with energy providers all around the world—wherever Sun has engineering, manufacturing, distribution, sales, or service locations—to verify that we can depend on the delivery and quality of power supply. Because the majority of our facilities require continuous, high-quality electric power, we have encouraged energy providers to simulate the Y2K transition within their planning, supervisory control, metering, dispatching, and generation systems.

Y2K has also engendered an unusual collaboration for our facilities in California's Silicon Valley. Every two months for the last 18 months we have met with other locally based high-tech manufacturers—such as Hewlett Packard, Intel, and Cisco—to discuss our common concerns and to review contingency plans. While we are fierce competitors in the marketplace, we all recognize the mutual benefit in working together on this issue. Y2K has been a big equalizer.

Manufacturing production is a top priority in Sun's Y2K preparedness efforts.

Courtesy of Sun Microsystems, Inc.

Also included in these meetings have been representatives from local governments and the power and telephone companies. As high-tech manufacturers see it, the greatest potential electric power problem has to do with availability, rather than degradation in power quality. And most energy providers now consider themselves to be "Y2K-ready" on both counts.

While Y2K is a great news story, my feeling is that any power problems that do result from the date transition will be of the minor or "nuisance" variety. But I would bet there will be no change in the electric power supplied. ∎

Dennis Symanski is manager of compliance engineering at Sun Microsystems, Inc. (*http://www.sun.com/*) in Menlo Park, California. He contributed the lead article, "What's Ahead for Commercial Technologies," to the Fall 1996 issue of *Signature* (NL-107026).
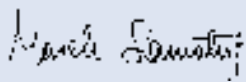
who will face these problems are not familiar with the principles of EMC.

Our growing dependence on microprocessors will spawn new EMC issues that need attention from the research community and the electric enterprise. Examples include sensitive electronic systems such as global positioning for land surveying systems, wireless communications systems that depend on embedded microprocessors, and even interference from distribution lines to railroad or pipeline operations.

Ushered in with Y2K problems, an endless stream of new devices and technologies are practically certain to perpetuate EMC challenges in the new millennium.

Marek Samotyj, Manager
EPRI Power Quality Product Line

to respond to a problem should be identifiable to explain and, if necessary, to defend their actions.

10. *Regular Monitoring and Proper Scheduling*. Individuals with responsibility should submit regular reports to their superiors on progress made in resolving Y2K issues. This ensures proper communications with affected persons and allows those with decision-making responsibility to respond quickly if circumstances require. Most energy providers have deadlines for testing and final responses related to Y2K issues. A good faith effort that does not meet a given deadline, along with communication to potentially affected persons, will likely not result in liability. However, failure to have a schedule for compliance and a resulting inability to track the rate of performance could be found to be unreasonable under the circumstances.

Reducing Exposure

In addition to addressing activities that can pose liability concerns, energy providers should review whether their company is utilizing appropriate measures to reduce liability exposures due to Y2K. Monitoring federal and state legislation is important, as they may provide protection from Y2K liability. The fundamental tools for reducing exposure are

- Contractual limitations of liability, by which parties agree who is responsible for different types of losses, what standard of care

will be used for measuring their actions, and what types of damages can be recovered in the event of a power disturbance;

- Governmental and other legal "safe harbors," which protect the parties from liability; and

- Insurance coverage, both current and pre-existing, which potentially provides sufficient limits without exclusions or other terms that may prevent recovery.

Finally, doing the right thing will not be a good defense to assertions of liability at trial unless energy providers can *prove* that they did the right thing. Therefore, they should take measures now to protect evidence that could clear any guilt or blame, and to maintain contact with important witnesses.

Most legal professionals expect some litigation involving Y2K-related issues. Since no one can predict who will be sued or the level of damages that may be awarded, it is a good idea to focus now on the factors that may influence those lawsuits. It is not too late to alter current practices to protect against potential legal exposure. ∎

Barry J. Fleishman is a partner with the law firm of Dickstein Shapiro Morin & Oshinsky LLP (*http://www.dsmo.com/*) in Washington, DC. He has written numerous articles on power quality and related liability and insurance issues. The opinions expressed in this paper are those of the author and not necessarily those of his firm or any of his clients.

EPRI

NL-113032-OL